Research on ARP Attack and Defense

Lan Haoliang, Gao Gugang, Xu Jie, Xue Yishi, Ma Zhuo
Department of Computer Information and Network Security, Jiangsu Police Institute, Nanjing, Jiangsu, China

Abstract: The network anomalies, illegal control, data theft and tampering caused by ARP attack have made ARP attack and defense a focus in the field of network security. In response to the common ARP attack in local area networks, the paper first analyzes the ARP protocol and its shortcomings. On this basis, the basic principles and common simulation methods of ARP attack were elaborated. Finally, the current mainstream ARP attack detection and defense methods were discussed in conjunction with network management.

Keywords: ARP Protocol; Local Area Network; Attack Detection; Attack Prevention

1. Introduction

The design of network architecture and the protocols built upon it is crucial for network security. Correspondingly, many current network attacks are caused by design flaws in the related network protocols under the TCP/IP architecture, with the Address Resolution Protocol (ARP) attack[1] being a typical example. As a standard protocol within local area networks, ARP has been in use since its proposal in 1982, and ARP attacks are therefore widespread in current local area networks. Such attacks can lead to network anomalies, illegal control, data theft, and tampering, among other adverse consequences. To effectively curb ARP attacks, Jin Yebing et al.[2] proposed an optimized ARP attack protection scheme by combining VLAN technology on layer 3 switches. Zhang Yuanyuan et al.[3] used IP/MAC bidirectional binding to defend against ARP attacks and spoofing, thereby preventing network outages. Yu Long et al.[4] regularly read ARP, VLAN, MAC-PORT, and other information from core switches based on the SNMP protocol, and used this information combined with a comprehensive detection algorithm to promptly detect, locate, and handle ARP attacks. Wang Li et al.[5] summarized the update patterns of ARP mapping tables based on ARP attack simulations and proposed a real-time ARP attack detection and recovery method using SNMP and WinPcap. Cheng Yanyan[6] proposed a method based on dynamic fingerprint detection and probability detection to effectively curb data leakage after ARP attacks. Song Yu et al.[7] proposed an industrial control system ARP attack intrusion detection method based on convolutional neural networks and bidirectional long short-term memory networks. Chen Yong et al.[8] used Markov chain isomorphism to obtain the relationship curve between the implementation rate of LTE-R three-level clock nodes under ARP attacks and the normal and abnormal synchronization of the PTP protocol, providing a reference for effectively improving the safety and operational efficiency of high-speed railways.

In summary, research on ARP attacks has always been a focus in the field of network security. Therefore, it is necessary to comprehensively discuss ARP attacks to help network security professionals systematically and deeply understand their basic principles, master common attack forms and defense measures, and better maintain network security. Specifically, this paper first introduces the ARP protocol and the basic principles of ARP attacks. On this basis, it summarizes common simulation methods for ARP attacks. Finally, it discusses in detail the current detection, defense, and troubleshooting of ARP attacks.

2. Address Resolution Protocol

2.1 Resolution Process

Data packets in the network need to be forwarded layer by layer through intermediate devices from the source to the destination. This forwarding relies mainly on IP addresses at the network layer and MAC addresses (physical

addresses) at the data link layer. Correspondingly, ARP is primarily a protocol that maps IP addresses to MAC addresses. The specific address resolution process is shown in Figure 1. Suppose host A in the same network segment sends data to host B. Host A will first check its ARP table. If it contains the MAC address corresponding to host B, host A will directly use this MAC address to complete the frame encapsulation and transmission of the IP data packet. Conversely, if host A's ARP table does not cache the mapping of host B's IP address to its MAC address, host A can obtain this mapping relationship based on the ARP protocol through the following process:

(1) Host A caches the IP data packet and then broadcasts an ARP request message containing host A's IP address, host A's MAC address, host B's IP address, and host B's MAC address as all zeros. All hosts in this network segment will receive this ARP request and check whether they are the target of the request message through the IP address. Therefore, only host B will respond to the request.

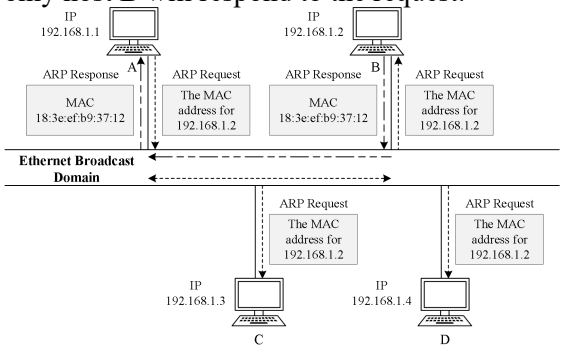

Figure 1. ARP Address Resolution Process

(2) Host B first stores the mapping of host A's IP address and MAC address as a new entry in its ARP table, and then sends an ARP response message containing its own MAC address to host A in unicast mode.

(3) After receiving the ARP response, host A will insert the mapping of host B's IP address and MAC address into its ARP table, and then use host B's MAC address as the destination address to encapsulate the IP data packet and send it out through the corresponding port.

The ARP table, as an important data structure, can limit the number of network broadcasts and accelerate data packet forwarding. It can be further divided into dynamic ARP tables and static ARP tables. The dynamic ARP table is automatically generated and maintained based on the ARP protocol through ARP messages. Its entries are subject to aging, updating, and being overwritten by static ARP entries. The static ARP table is manually configured and maintained, does not age or get overwritten, and can prevent ARP attacks to a certain extent, ensuring communication security. Additionally, users can view their device's ARP cache table, as shown in Figure 2, using the ARP -a command.

```
C:\Users\lan>arp -a
Interface: 172.18.1.54 --- 0x16
  Internet Address      Physical Address      Type
  172.18.0.1            58-69-6c-63-c5-f4     Dynamic
  224.0.0.2             01-00-5e-00-00-16     Static
  224.0.0.251           01-00-5e-00-00-fb     Static
  239.255.255.250       01-00-5e-7f-ff-fa     Static
  255.255.255.255       ff-ff-ff-ff-ff-ff     Static
```

Figure 2. ARP Cache Table

2.2 Protocol flaws

The smooth operation of ARP is based on the mutual trust of hosts within the same network segment. However, this is often not the case in real networks, as malicious nodes often exploit the broadcast nature, statelessness, lack of authentication, and other characteristics of the ARP protocol to launch ARP attacks.

Broadcast: ARP request messages are received by all hosts in the same network segment. Even if the receiving host is not the actual target host, it can still send an ARP response message.

Statelessness: Any host in the same network segment will unconditionally receive ARP request and response messages without sending an ARP request, thereby updating its ARP table entries.

Lack of Authentication: Since the ARP protocol assumes that all hosts in the same network segment are trustworthy, it does not verify the authenticity and validity of the IP address to MAC address mapping.

Disorderliness: Unlike general logic, ARP requests and responses are not distinguished by order, meaning that requests and responses do not need to be logically associated

3. ARP Attack

Due to the inherent design flaws of ARP, its protocol vulnerabilities are often exploited for network attacks. This section introduces the basic principles of ARP attacks and elaborates on common simulation methods for ARP attacks.

3.1 Attack Principle

The basic principle of ARP attacks is to intercept network traffic data or cause network interruptions by forging request or response messages. These attacks can be further divided into man-in-the-middle spoofing and network interruption types.

3.1.1 Man-in-the-middle spoofing

Man-in-the-middle spoofing attacks do not cause network interruptions. Their purpose is to intercept normal communication traffic, but the communication fluency is affected to some extent due to the additional forwarding. Additionally, depending on the object the attacking host impersonates, this type of attack can be further divided into gateway spoofing and host spoofing. As shown in Figure 3, in gateway spoofing, the attacking host B sends ARP response messages containing the gateway's IP address and its own MAC address to other hosts in the same network segment, while also sending ARP response messages containing other hosts' IP addresses and its own MAC address to the gateway. Similarly, in host spoofing, the attacking host B sends response messages containing false information to hosts A and C

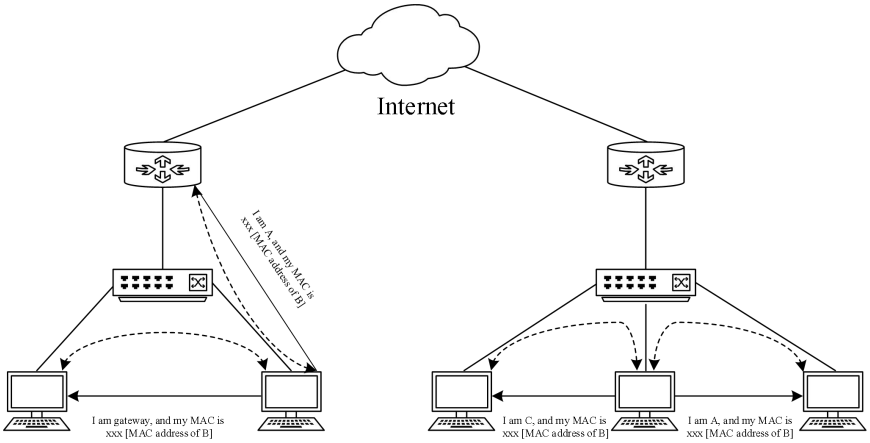

Figure 3. Man-in-the-Middle Spoofing

3.1.2 Network interruption

The purpose of network interruption ARP attacks is not to intercept network traffic but to interrupt the normal network access of other hosts in the network segment through the attack. As shown in Figure 4, in network interruption attacks, the attacking host B sends false ARP response messages containing virtual MAC addresses, resulting in unreachable destinations and causing network interruptions.

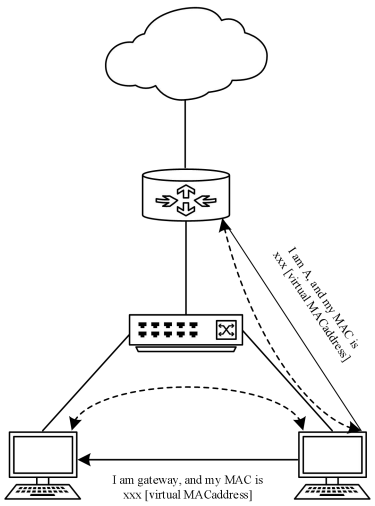

Figure 4. Network Interruption

3.1.3.Attack simulation

Based on understanding the basic principles of ARP attacks, simulating ARP attacks can deepen the understanding and mastery of these principles. Currently, ARP attack simulations are mainly implemented using software simulation platforms such as eNSP, “Network Law Enforcer,” and Packet Tracer[9-11] or real local area network environments[12], combined with different attack forms.。

(1) ARP flood attack simulation: This type of attack simulation mainly involves sending a large number of false ARP request or response messages to the gateway or host in a short period (at a rate of about 1000 per second), causing the normal ARP table entries of the attacked host or gateway to be overwritten or the ARP table to overflow, making it impossible for users to access the network normally.

(2) ARP denial of service attack simulation: This type of attack simulation mainly involves sending a large number of invalid ARP request packets to the switch, wasting a large amount of system resources on processing ARP MISS data packets, thereby disrupting its normal

service.
(3) ARP man-in-the-middle spoofing attack simulation: This attack uses false ARP messages containing the attacker's MAC address and the target's IP address to simulate the role of a man-in-the-middle, thereby achieving network traffic interception. Therefore, the key to simulation lies in the bidirectional spoofing between the gateway and the target or between the target and the target.
(4) ARP network interruption attack simulation: This type of attack simulation mainly uses false ARP messages containing virtual MAC addresses and the target's IP address to achieve the purpose of interrupting network services. Therefore, the key to simulation lies in using virtual MAC addresses to fill the target's ARP cache table.

4. ARP Attack Detection And Defense

Due to the strong concealment of ARP attacks, their harm to hosts in local area networks is usually significant. Therefore, from the perspective of network management, ARP protection in real network environments generally involves two aspects: ARP attack detection and ARP attack defense.

4.1 Attack Detection

(1) Real-time monitoring based on SNMP: The detection server uses a comprehensive detection algorithm[4] and the SNMP protocol to regularly read ARP, VLAN, MAC-PORT, and other information to monitor and locate ARP attack behaviors in real-time, thereby taking different technical measures based on the actual network situation.
(2) ARP table analysis: ARP attacks inevitably cause abnormal changes in the ARP cache table. Therefore, the content of the ARP table can be detected and analyzed based on the basic principles of ARP attacks. For example, if multiple IPs correspond to the same MAC in a network segment, an attack can be inferred.
(3) Packet capture analysis based on WinPcap: Use WinPcap to capture ARP response packets in the network, analyze and discover suspicious behaviors based on attack logic[5], thereby determining the MAC address of the attacking host and its corresponding port, and blocking the ARP attack behavior in time.

4.2.Attack Defense

(1) IP-MAC static binding: Use specific commands to bind the IP address and MAC address bidirectionally on the host or router to resist ARP attacks from changing ARP table entries. This method also has some shortcomings. For example, if there is a DHCP service in the network that causes the IP address to change dynamically, the host may not be able to access the network normally.
(2) VLAN Division: Creating multiple subnets within the local area network using VLAN technology can effectively isolate ARP broadcast packets within the local area network, thereby narrowing the scope of ARP attacks, improving network security, and facilitating later ARP attack troubleshooting.
(3) ARP Firewall: Enabling an ARP firewall on the host can effectively prevent ARP attacks. Correspondingly, if an ARP attack occurs in this case, the network and system overhead will also increase.
(4) Specific Software: Run specific software to monitor and correct suspicious ARP traffic in the network, such as running “ARP SERVER” at specific intervals to broadcast the correct IP-MAC mapping relationships of all hosts in the network segment.

5. Conclusion

This paper comprehensively discusses ARP attacks and defenses based on current research. It specifically analyzes the vulnerabilities and flaws of the ARP protocol, summarizes the principles, forms, simulations, detection, and defense methods of ARP attacks, and strives to provide references for learning and conducting related research on ARP attacks.

Acknowledgments

This paper is supported by Jiangsu police institute education and teaching reform research project (No. 2023A16), Jiangsu social science application research excellence project (No. 23SYC-127), Jiangsu university philosophy and social science pesearch general project (No. 2022JYB0471), Jiangsu police institute key project of natural science pesearch (No. 2022SJYZZ05).

References

[1]Gouda M G, Huang C T. A secure address resolution protocol[J]. Computer Networks, 2003, 41(1): 57-71.
[2]Jin Yebing, Xia Yang. ARP attack and

protection in large local area networks[J]. Microcomputer Information, 2009, 25(06): 101-102.

[3]Zhang Yuanyuan, Hou Jiantao. The principles and solutions of ARP attacks and ARP spoofing[J]. Coal Technology, 2010, 29(11): 199-200.

[4]Yu Long, Zhu Huiming, Tian Shengwei, et al. Research on ARP attack detection methods in campus networks based on SNMP[J]. Computer Applications and Software, 2011, 28(05): 120-122.

[5]Wang Li, Li Yusheng, Hu Lewei. Real-time detection and recovery of ARP attacks based on SNMP and WinPcap[J]. Science and Technology Bulletin, 2012, 28(06): 78-79.

[6]Cheng Yanyan. Network data leakage prevention method after ARP attacks[J]. Science Technology and Engineering, 2017, 17(34): 273-277.

[7]Song Yu, Li Zhilin, Cheng Chao. Industrial control system ARP attack intrusion detection method based on CNN-BILSTM[J]. Computer Applications Research, 2020, 37(S2): 242-244.

[8]Chen Yong, Zhan Zhixian, Liu Wen. Vulnerability analysis of the next-generation high-speed railway LTE-R time synchronization network protocol[J]. Journal of the China Railway Society, 2023, 45(01): 63-74.

[9]Qiu Hong, Shi Junyu, Tu Qiuyue. Analysis of ARP attacks and protection in local area networks[J]. Computer and Network, 2021, 47(01): 56-59.

[10]Wang Xiangyu, Qiu Chunrong. Experimental design based on "ARP attack and defense" course[J]. Laboratory Research and Exploration, 2009, 28(05): 175-177.

[11]Xu Dawei, Dai Cheng, Zhu Liehuang, et al. Solutions and examples of ARP attacks under SDN architecture[J]. Journal of Guangzhou University (Natural Science Edition), 2021, 20(04): 63-75.

[12]Pan Jiafu. Principle analysis and countermeasure research of ARP attacks[J]. Software Engineering, 2019, 22(05): 25-31.

